Chen *et al. Research in Number Theory* (2015) 1:28
DOI 10.1007/s40993-015-0028-0

Research in Number Theory
a SpringerOpen Journal

RESEARCH Open Access

Linnik's theorem for Sato-Tate laws on elliptic curves with complex multiplication

Evan Chen[1*], Peter S. Park[2] and Ashvin A. Swaminathan[3]

*Correspondence:
evanchen@mit.edu
[1] Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139, United States of America
Full list of author information is available at the end of the article

Abstract

Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication (CM), and for each prime p of good reduction, let $a_E(p) = p + 1 - \#E(\mathbb{F}_p)$ denote the trace of Frobenius. By the Hasse bound, $a_E(p) = 2\sqrt{p}\cos\theta_p$ for a unique $\theta_p \in [0, \pi]$. In this paper, we prove that the least prime p such that $\theta_p \in [\alpha, \beta] \subset [0, \pi]$ satisfies

$$p \ll \left(\frac{N_E}{\beta - \alpha}\right)^A,$$

where N_E is the conductor of E and the implied constant and exponent $A > 2$ are absolute and effectively computable. Our result is an analogue for CM elliptic curves of Linnik's Theorem for arithmetic progressions, which states that the least prime $p \equiv a \pmod q$ for $(a, q) = 1$ satisfies $p \ll q^L$ for an absolute constant $L > 0$.

1 Introduction

Let E be an elliptic curve over $\mathbb{Q}$, and for each prime p, let $\#E(\mathbb{F}_p)$ be the number of rational points of E over the finite field $\mathbb{F}_p$. Taking $a_E(p) = p + 1 - \#E(\mathbb{F}_p)$ to be the trace of Frobenius as usual, we recall the following important result of Hasse, which holds when E has good reduction at p:

$$\left|a_E(p)\right| \le 2\sqrt{p}.$$

It follows that for each prime p, there is a unique angle $\theta_p \in [0, \pi]$ (which we call the "Sato-Tate" angle) such that $a_p = 2\sqrt{p}\cos\theta_p$. For a fixed elliptic curve E, it is natural to study the distribution of the angles θ_p as p ranges across the primes at which E has good reduction. The now-proven Sato-Tate Conjecture provides an asymptotic for this distribution that depends on whether or not E has complex multiplication (CM). While the CM case was established by Hecke, the non-CM case was recently proven in [1] by Barnet-Lamb, Geraghty, Harris, and Taylor.

Theorem (Sato-Tate Conjecture)**.** Fix an elliptic curve $E/\mathbb{Q}$, and let $I = [\alpha, \beta] \subset [0, \pi]$ be a subinterval. Then we have that

$$\lim_{x\to\infty} \frac{\#\{p \le x : \theta_p \in I\}}{\#\{p \le x\}} = \begin{cases} \int_I \frac{2}{\pi}\sin^2\theta\, d\theta & \text{if } E \text{ is non-CM,} \\ \frac{\delta_I}{2} + \frac{\beta-\alpha}{2\pi} & \text{if } E \text{ is CM} \end{cases}$$

where $\delta_I = 1$ if $\pi/2 \in I$ and $\delta_I = 0$ otherwise.

Because the Sato-Tate conjecture provides an equidistribution result for the angles θ_p in a given subinterval $I \subset [0, \pi]$, it is natural to ask whether one can determine the *least* prime p such that $\theta_p \in I$. In this paper, we address the CM case of this question by proving the following theorem:

Theorem 1.1. *Let $E/\mathbb{Q}$ be a CM elliptic curve of conductor N_E. There exists a prime p such that $\theta_p \in I$ and*

$$p \ll \left(\frac{N_E}{\beta - \alpha}\right)^A,$$

where the implied constant and exponent $A > 2$ are absolute and effectively computable.

Observe that Theorem 1.1 is analogous to Linnik's Theorem, which provides an upper bound on the least prime in an arithmetic progression. Specifically, Linnik showed in [11, 12] that the least prime $p \equiv a \pmod{q}$, for relatively prime integers a and q, satisfies $p \ll q^L$ (where the implied constant and the exponent $L > 0$ are absolute and effectively computable). This analogy between Theorem 1.1 and Linnik's Theorem is reasonable to expect; indeed, the least prime p with $\theta_p \in I$ should grow inversely with the length of I and should depend in some way on the arithmetic properties of E (such as its conductor), just as the least prime p in an arithmetic progression modulo q should grow with q.

Remark. The non-CM analogue of Theorem 1.1 was proven by Lemke Oliver and Thorner in [10]. Their bound depends on the number of symmetric-power L-functions of E that are known to have analytic continuations and functional equations of the usual type.

Also, it is well-known that for a given elliptic curve $E/\mathbb{Q}$, the traces of Frobenius $a_E(p)$ are the p^{th} Fourier coefficients of a weight 2 newform of level N_E. One can thus formulate this problem in the more general context of newforms of even weight $k \geq 2$ with complex multiplication; the proof is essentially the same as the proof of Theorem 1.1. □

The rest of this paper is organized as follows. Section 2 presents an introduction to the analytic theory of CM elliptic curves and L-functions associated to Hecke Grössencharaktere, which are the fundamental tools that we employ in our proof of Theorem 1.1. Then, Section 3 employs the tools developed in Section 2 to give a detailed proof of Theorem 1.1.

2 CM elliptic curves and Hecke *L*-functions

In this section, we provide a brief description of the relevant facts about CM elliptic curves over $\mathbb{Q}$ and L-functions of Hecke Grössencharaktere that are employed in our proof of Theorem 1.1; a standard reference is [5]. Note that throughout the rest of the paper, all implied constants are absolute unless otherwise specified.

Let $K/\mathbb{Q}$ be an algebraic number field, and let $\mathfrak{m} \subset \mathcal{O}_K$ be a nonzero integral ideal. Let ξ denote a Hecke Grössencharakter over K of modulus $\mathfrak{m}$ and frequency k. When K is an imaginary quadratic field, every Hecke Grössencharakter can be thought of as the product of a ray-class character $\chi : (\mathcal{O}_K/\mathfrak{m})^* \to S^1$ with an angle character $\chi_\infty : \mathbb{C}^* \to S^1$, where

$S^1 = \{z \in \mathbb{C} : |z| = 1\}$. (Here, by frequency of ξ, we mean the frequency of χ_∞. See [6] for details.) The Hecke L-function $L(s,\xi)$ associated to ξ is defined as the Euler product

$$L(s,\xi) = \prod_{\mathfrak{p}\subset\mathcal{O}_K} (1 - \xi(\mathfrak{p})\boldsymbol{N}(\mathfrak{p})^{-s})^{-1},$$

which converges absolutely for $\sigma > 1$. Hecke showed that the above product can be meromorphically continued to the entire complex plane, giving an L-function whose degree equals $[K : \mathbb{Q}]$. Furthermore, he proved that $L(s,\xi)$ is entire if ξ is nontrivial and that $L(s,\xi)$ has a simple pole at $s = 1$ when ξ is trivial.

As described in [2] and [15], the theory of Hecke Grössencharaktere is fundamental to the study of CM elliptic curves. Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E, and suppose that E has complex multiplication by the ring of integers $\mathcal{O}_K$ of a number field $K/\mathbb{Q}$ with absolute discriminant $|d_K|$. Recall that in this case, K is necessarily an imaginary quadratic field of class number 1, so that $\mathcal{O}_K$ is a principal ideal domain. For prime ideals $\mathfrak{p} \subset \mathcal{O}_K$ at which E has good reduction, set

$$a_E(\mathfrak{p}) = \boldsymbol{N}(\mathfrak{p}) + 1 - \#E(\mathbb{F}_\mathfrak{p})$$

where $\mathbb{F}_\mathfrak{p} := \mathcal{O}_K/\mathfrak{p}$. Then, the Hasse bound tells us that

$$|a_E(\mathfrak{p})| \le 2\sqrt{\boldsymbol{N}(\mathfrak{p})}.$$

Thus, for each prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ at which E has good reduction, we can define $\theta_\mathfrak{p} \in [0,\pi]$ such that $a_\mathfrak{p} = 2\sqrt{\boldsymbol{N}(\mathfrak{p})}\cos\theta_\mathfrak{p}$. Now, consider a totally multiplicative map ξ_E that is defined on unramified prime ideals $\mathfrak{p} \subset \mathcal{O}_K$ by

$$\xi_E(\mathfrak{p}) = \exp\left(\pm i\theta_\mathfrak{p}\right)$$

where the symbol "$\pm$" indicates a sign that depends on $\mathfrak{p}$ and E. It is a well-known result of Weil (see [16]) that if the signs $\pm$ are chosen appropriately for each $\mathfrak{p}$, then ξ_E is a Hecke Grössencharakter over K. We note that ξ_E has frequency 1, and as discussed in [14], the modulus $\mathfrak{m}$ of ξ_E has norm $\boldsymbol{N}(\mathfrak{m}) = N_E/|d_K|$. For $k \in \mathbb{Z}\setminus\{0\}$, we denote by ξ_E^k the map defined by $\xi_E^k(\mathfrak{a}) := \xi_E(\mathfrak{a})^k$ for nonzero ideals $\mathfrak{a} \subset \mathcal{O}_K$; observe that this is a Hecke Grössencharakter of modulus $\mathfrak{m}$ and frequency k.

Taking the analytic conductor $\mathfrak{q}(s,\xi)$ of an L-function $L(s,\xi)$ to be defined as in Equation 5.7 of [6], it is easy to deduce the following useful bound on the analytic conductor of $L\left(s,\xi_E^k\right)$:

$$\log\mathfrak{q}\left(s,\xi_E^k\right) \ll \log\left((|s|+3)\cdot\boldsymbol{N}(\mathfrak{m})\cdot k\right). \tag{2.1}$$

We devote the remainder of this section to presenting a few relevant results on the distribution of nontrivial zeros of Hecke L-functions; we will apply these results in Section 3 to $L\left(s,\xi_E^k\right)$. The following lemma, which is adapted from Theorem 5.10 in [6], provides a zero-free region for Hecke L-functions over quadratic fields of class number 1.

Lemma 2.1. *Let K be a quadratic number field of class number 1, let $\mathfrak{m} \subset \mathcal{O}_K$ be a nonzero integral ideal, and let ξ be a Hecke Grössencharakter modulo $\mathfrak{m}$. Then $L(s,\xi)$ has at most one zero in the region*

$$\sigma \ge 1 - \frac{c_1}{\log\mathfrak{q}(it,\xi)}$$

for some absolute constant $c_1 > 0$. The exceptional "Siegel zero" can only exist if ξ is a real quadratic character and is necessarily both real and simple.

Note that the region defined in Lemma 2.1 is free of zeros when the Hecke Grössencharakter is trivial or has infinite order. Since the character ξ_E^k is trivial if $k = 0$ and has infinite order if $k \neq 0$, we need not consider Siegel zeros in applying Lemma 2.1 to $L\left(s, \xi_E^k\right)$. The next lemma, which is adapted from part (1) of Proposition 5.7 in [6], provides an estimate on the vertical distribution of zeros of Hecke L-functions over quadratic fields:

Lemma 2.2. *Retain the setting of Lemma 2.1. For any $t \geq 2$, the number of zeros ρ of $L(s, \xi)$ with $\gamma \in [t-1, t+1]$ is less than*

$$c_2 \log \mathfrak{q}(it, \xi)$$

for some absolute constant c_2.

A key input into the proof of Linnik-type theorems is a logarithm-free zero-density estimate. In our proof of Theorem 1.1, we will employ the following estimate, which we have adapted from [3]:

Lemma 2.3. *Fix an integer $H \geq 1$, an imaginary quadratic number field K of class number 1, and a nonzero integral ideal $\mathfrak{m} \subset \mathcal{O}_K$. Consider the product*

$$L(s; \mathfrak{m}, H) = \prod_{\xi} L(s, \xi),$$

where ξ ranges over all Hecke Grössencharaktere with modulus $\mathfrak{m}$ and frequency at most H. Let $N(\lambda, T)$ denote the number of zeros of $L(s; \mathfrak{m}, H)$ that lie in the rectangle

$$1 - \lambda < \beta < 1 \quad \text{and} \quad |\gamma| \leq T.$$

Then there exists an absolute constant $c_3 \in (0, 1)$ and an absolute constant c_4 such that if $\lambda \in (0, c_3)$ and $T \geq N(\mathfrak{m})(1 + H)$, then

$$N(\lambda, T) \leq T^{c_4 \lambda}.$$

Remark. Similar zero-density estimates were obtained by Koval'čik in [9]. These density estimates are unlikely to produce Linnik-type theorems because they are not logarithm-free. However, they do have applications in studying primes of the form $p = a^2 + b^2$ where $|b| < p^{1/4+\epsilon}$ and in producing an analogue of the Bombieri-Vinogradov theorem for primes $p = a^2 + b^2$ where $\arg(a + bi)$ lies in a given sector. We thank Professor Jean-Pierre Serre for introducing us to this paper. □

3 Proof of Theorem 1.1

In this section, we provide a complete proof of the main result in this paper, namely Theorem 1.1. Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E with CM by $\mathcal{O}_K$, where K is necessarily an imaginary quadratic field of class number 1. Recall from Section 2 that we can associate to E a Hecke Grössencharakter ξ_E over K of modulus $\mathfrak{m} \subset \mathcal{O}_K$ and frequency 1. Fix a subinterval $I = [\alpha, \beta] \subset [0, \pi]$ with indicator function denoted by χ_I, and put

$$x = \frac{\boldsymbol{N}(\mathfrak{m})}{\beta - \alpha}. \tag{3.1}$$

Notice that x has a positive lower bound of $1/\pi$, and recall that

$$\frac{\boldsymbol{N}(\mathfrak{m})}{\beta - \alpha} = \frac{N_E}{|d_K|(\beta - \alpha)} \leq \frac{N_E}{\beta - \alpha}.$$

Thus, to prove Theorem 1.1, it suffices to show that if x is sufficiently large, we can pick a constant $A > 2$ so that there exists a prime $p \ll x^A$ with $\theta_p \in I$. The method we employ in this section is based on the work of Graham and Jutila on computing explicit Linnik constants (see [4, 7]) as well as that of Kaufman (see [8]).

3.1 Initial setup of the proof

Let $A > 2$ be a sufficiently large absolute constant. Let $R : (0, \infty) \to \mathbb{R}$ be supported on $[x^{A-2}, x^A]$. Consider the sum S defined by

$$S := \sum_{\substack{\mathfrak{p} \subset \mathcal{O}_K \\ f_{\mathfrak{p}} = 1}} \frac{\log \boldsymbol{N}(\mathfrak{p}) R(\boldsymbol{N}(\mathfrak{p})) \chi_I(\theta_{\mathfrak{p}})}{\boldsymbol{N}(\mathfrak{p})}. \tag{3.2}$$

Here, the sum is taken over unramified prime ideals $\mathfrak{p}$ (henceforth all sums over primes will implicitly be taken over unramified primes). By $f_{\mathfrak{p}}$ we mean the *inertial degree* of $\mathfrak{p}$, which is the degree of $\mathcal{O}_K/\mathfrak{p}$ as an $\mathbb{F}_p$-vector space (recall that $\boldsymbol{N}(\mathfrak{p}) = p^{f_{\mathfrak{p}}}$). In our case, since K is a quadratic field, we have $f_{\mathfrak{p}} \in \{1, 2\}$. We will show that $S > 0$.

As in [4], we construct the function $R(y)$ by means of a kernel. For $s \in \mathbb{C}$, define a kernel[1] $K(s)$ by

$$K(s) := x^{\frac{A-2}{2} \cdot s} \left(\frac{x^s - 1}{s \log x} \right),$$

and take the function $R(y)$ to be given by

$$R(y) := \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} K(s)^2 y^{-s} \, ds. \tag{3.3}$$

As stated in [4, 7], the function $R(y)$, as defined above, vanishes outside of the interval $[x^{A-2}, x^A]$ and satisfies $R(y) \ll (\log x)^{-1}$ when $y \in [x^{A-2}, x^A]$. We will utilize the following bound on our function $K(s)$:[2]

Lemma 3.1 (Graham, [4]). *Let $B_1 = A - 2$. For $\sigma < 0$, we have that*

$$|K(s)|^2 \leq x^{B_1 \sigma} \min \left(1, \frac{4}{|s|^2 (\log x)^2} \right).$$

3.2 Estimating *S*

In order to rephrase our problem into one that concerns the Hecke Grössencharaktere ξ_E^k, we use the following lower approximation to χ_I with symmetric, compactly supported Fourier coefficients:

Lemma 3.2. *Let $I = [\alpha, \beta] \subset [0, \pi]$ be a subinterval, and let $M \in \mathbb{Z}_{>0}$. There exists a trigonometric polynomial*

$$S_{I,M}(\theta) = \sum_{|n| \leq M} b_n \exp(in\theta)$$

satisfying the following properties: For all $\theta \in [0,\pi]$, *we have* $S_{I,M}(\theta) \leq \chi_I(\theta)$, *and for all* $n \in \{-M,\ldots,M\} \setminus \{0\}$ *we have that* $b_n = b_{-n}$ *and that*

$$\left| b_0 - \frac{\beta-\alpha}{\pi} \right| \leq \frac{2}{M+1} \text{and } |b_n| \leq \left(\frac{2}{M+1} + \min\left\{ \frac{\beta-\alpha}{\pi}, \frac{2}{\pi|n|} \right\} \right). \tag{3.4}$$

Proof. The lemma follows by modifying the Beurling-Selberg minorant polynomials (see [13], §1.2, p. 5–6, for a formal definition of these polynomials) to be even and periodic modulo 2π. □

We are now in a position to estimate the indicator function χ_I of the interval $I = [\alpha,\beta] \subset [0,\pi]$ in terms of the Hecke Grössencharaktere ξ_E^k. We set $M = x^{1+\varepsilon}$ for an absolute $\varepsilon \in (0,1/2)$. From Lemma 3.2, we find that for each unramified prime ideal $\mathfrak{p} \subset \mathcal{O}_K$,

$$\chi_I(\theta_{\mathfrak{p}}) \geq \sum_{|k|\leq M} b_k \exp(ik\theta_{\mathfrak{p}}) = b_0 + \sum_{\substack{|k|\leq M \\ k\neq 0}} b_k \xi_E^k(\mathfrak{p}),$$

where the Fourier coefficients b_k satisfy the conditions specified in (3.4). Applying this lower approximation to χ_I to (3.2), we obtain the following estimate on S:

$$S = \sum_{f_{\mathfrak{p}}=1} \frac{\log \boldsymbol{N}(\mathfrak{p}) R(\boldsymbol{N}(\mathfrak{p}))\chi_I(\theta_{\mathfrak{p}})}{\boldsymbol{N}(\mathfrak{p})} \geq \sum_{f_{\mathfrak{p}}=1} \sum_{|k|\leq M} b_k \frac{\log \boldsymbol{N}(\mathfrak{p}) R(\boldsymbol{N}(\mathfrak{p}))\xi_E^k(\mathfrak{p})}{\mathrm{N}(\mathfrak{p})}.$$

Since $R(y)$ is nonzero for only finitely many integers y, the sum over primes in the right-hand-side of the above inequality is a finite sum. Thus, we can exchange the order of summation to conclude that

$$S \geq \sum_{|k|\leq M} b_k S_k, \qquad S_k = \sum_{f_{\mathfrak{p}}=1} \frac{\log \boldsymbol{N}(\mathfrak{p}) R(\boldsymbol{N}(\mathfrak{p}))\xi_E^k(\mathfrak{p})}{\boldsymbol{N}(\mathfrak{p})}. \tag{3.5}$$

In what follows, we denote the inner sum on the right-hand-side of (3.5) by S_k.

3.3 Estimating S_k

To estimate S_k using our knowledge of the Hecke L-function $L\left(s,\xi_E^k\right)$, we will introduce for every $k \in \{-M,\ldots,M\}$ an integral I_k defined as follows:

$$I_k := \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} K(s)^2 \left(-\frac{L'}{L}\left(s+1,\xi_E^k\right) \right) ds$$

Evaluating the logarithmic derivative of $L\left(s+1,\xi_E^k\right)$, we find that

$$-\frac{L'}{L}\left(s+1,\xi_E^k\right) = \sum_{\mathfrak{a}} \frac{\Lambda_K(\mathfrak{a})\xi_E^k(\mathfrak{a})}{\boldsymbol{N}(\mathfrak{a})^{s+1}}, \tag{3.6}$$

where Λ_K is the von Mangoldt function over the number field K, defined as

$$\Lambda_K(\mathfrak{a}) = \begin{cases} \log \boldsymbol{N}(\mathfrak{p}) & \text{if } \mathfrak{a} = \mathfrak{p}^m, \\ 0 & \text{otherwise.} \end{cases}$$

Substituting (3.6) into the definition of the integral I_k and integrating term by term, we obtain the following series representation of I_k:

$$I_k = \sum_{\mathfrak{a}} \frac{\Lambda_K(\mathfrak{a}) R(\boldsymbol{N}(\mathfrak{a}))\xi_E^k(\mathfrak{a})}{\boldsymbol{N}(\mathfrak{a})}. \tag{3.7}$$

Recall from (3.7) that I_k can be expressed as a sum over prime powers, whereas the desired sum S_k is a sum over primes $\mathfrak{p}$ with $f_\mathfrak{p} = 1$. We bound the difference between I_k and S_k as follows.

Lemma 3.3. *For any k we have* $|I_k - S_k| = O(x^{-2})$.

Proof. Recall the fact that $R(y) = 0$ for $y \notin [x^{A-2}, x^A]$, and moreover that $R(y) \ll (\log x)^{-1}$ for $y \in [x^{A-2}, x^A]$. Thus, when $N(\mathfrak{a}) \in [x^{A-2}, x^A]$, we have that

$$\left| \frac{\Lambda_K(\mathfrak{a}) R(\boldsymbol{N}(\mathfrak{a})) \xi_E^k(\mathfrak{a})}{\boldsymbol{N}(\mathfrak{a})} \right| \ll \frac{\log(x^A) \cdot (\log x)^{-1}}{x^{A-2}} = \frac{A}{x^{A-2}}.$$

The number N of nonzero terms in the sum (3.7) corresponding to ideals $\mathfrak{a} = \mathfrak{p}^k$ with $k > 2$ is at most twice the number of prime powers $\leq x^A$, so we have that $N \ll x^{A/2}$. Moreover, the number of prime ideals with $f_\mathfrak{p} = 2$ is also at most $x^{A/2}$ (since the norm of such a prime ideal is necessarily a perfect square). Thus, the difference between S_k and I_k can be bounded as follows:

$$|S_k - I_k| \ll \frac{A}{x^{A-2}} \cdot x^{A/2} \ll x^{-2}$$

provided that $A \geq 8$. □

On the other hand, we can evaluate the integral I_k by shifting the contour from $\sigma = 2$ to $\sigma = -5/4$.[3] To this end, we prove the following lemma:

Lemma 3.4. *We have that*

$$I_k = \delta(k) - \sum_\rho{}^k K(\rho - 1)^2 + O(x^{-2})$$

where the superscript "k" on the sum indicates that the sum is taken over nontrivial zeros ρ *of* $L\left(s, \xi_E^k\right)$ *and where* $\delta(k)$ *denotes the Kronecker delta function.*

Proof. Consider the truncated integral $I_k(T)$ defined for $T > 0$ by

$$I_k(T) := \frac{1}{2\pi i} \int_{2-iT}^{2+iT} K(s)^2 \left(-\frac{L'}{L}\left(s + 1, \xi_E^k\right) \right) ds,$$

where T does not coincide with the ordinate of a zero of $L\left(s, \xi_E^k\right)$. We want to shift the contour from

$$\sigma = 2 \quad \text{to} \quad \sigma = -5/4.$$

In doing so, the nontrivial zeros of $L\left(s + 1, \xi_E^k\right)$, which occur when $s + 1 = \rho$, contribute residues that sum to $-\sum_\rho{}^k K(\rho - 1)^2$. When $k = 0$, we know that $L\left(s, \xi_E^k\right)$ has a simple pole when $s + 1 = 1$, which contributes a residue of $\delta(k)$. Moreover, if $k = 0$, then $L\left(s, \xi_E^k\right)$ has a trivial zero at $s = -1$, which contributes a residue that is bounded by

$$\ll \frac{x^{2-A}(1 - x^{-1})^2}{(\log x)^2} \ll x^{-2}$$

provided that $A > 4$. It is easy to check that the integrand of I_k has no other poles in the range $-5/4 \leq \sigma \leq 2$. Thus, by the Residue Theorem, we have that

$$I_k(T) = \delta(k) - \sum_{\rho} K(\rho - 1)^2 + O(x^{-2}) + \frac{1}{2\pi i} \int_{\Gamma_T} K(s)^2 \left(-\frac{L'}{L}\left(s + 1, \xi_E^k\right)\right) ds$$

where Γ_T is the rectangular path consisting of the three legs

$$2 - iT \longrightarrow -\frac{5}{4} - iT \longrightarrow -\frac{5}{4} + iT \longrightarrow 2 + iT.$$

In order to evaluate the above integral, we require a bound on the logarithmic derivative of $L\left(s, \xi_E^k\right)$. To this end, one can obtain from (2.1), Lemma 2.2, and part (2) of Proposition 5.7 in [6] that for s satisfying $-\frac{1}{4} \leq \sigma \leq 3$ and $|t| = T$ sufficiently large, we have

$$\left| \frac{L'}{L}\left(s, \xi_E^k\right)\right| = O\left(\left(\log k(T + 3)\right)^2\right).$$

Note that the condition of having T sufficiently large can be removed if $\sigma = -5/4$, because $-5/4$ is bounded away from 0, 1, and all local parameters of $L\left(s, \xi_E^k\right)$ at infinity. This is important for estimating the integral along the vertical leg $\sigma = -\frac{5}{4}$ of Γ_T. Now, the integral along the first leg (horizontal leg at $t = -T$) is bounded in absolute value by

$$\ll \sup_{\substack{-\frac{5}{4} \leq \sigma \leq 2 \\ t = -T}} \left| x^{(A-2)s} \left(\frac{x^s - 1}{s \log x}\right)^2 \frac{L'}{L}\left(s + 1, \xi_E^k\right)\right| \ll \frac{x^{2(A-2)}(x^2 + 1)^2}{T^2} \left(\log k(T + 3)\right)^2,$$

which vanishes as $T \to \infty$. By an analogous argument, the integral along the third leg (horizontal leg at $t = T$) vanishes as $T \to \infty$. Finally, the integral along the second leg (the vertical leg at $\sigma = -5/4$) is bounded in absolute value by

$$\begin{aligned} &\ll \sup_{\substack{\sigma = -\frac{5}{4} \\ |t| \leq T}} \left| x^{(A-2)s} \left(\frac{x^s - 1}{\log x}\right)^2 \right| \int_{-T}^{T} \frac{\left(\log k(|t| + 3)\right)^2}{\left|-\frac{5}{4} + it\right|^2} dt \\ &\ll x^{-\frac{5}{4}(A-2)} \left(\frac{x^{-\frac{5}{4}} + 1}{\log x}\right)^2 \int_{-T}^{T} \frac{\left(\log k(|t| + 3)\right)^2}{\left|-\frac{5}{4} + it\right|^2} dt. \end{aligned}$$

Notice that as $T \to \infty$, the integral in the above expression converges by the p-test. Therefore, provided that $A > 6$, we have that the above term is $\ll x^{-2}$ in the limit as $T \to \infty$, which proves the lemma. □

3.4 Estimating the sum over zeros

We now combine our Fourier estimate of S with our estimate of S_k. By (3.5), Lemma 3.2 and the results of Section 3.3, we have

$$\begin{aligned} S \geq \sum_{|k| \leq M} b_k S_k &= \sum_{|k| \leq M} b_k (I_k + O(x^{-2})) \\ &= \sum_{|k| \leq M} b_k \left(\delta(k) - \sum_{\rho}{}^{k} K(\rho - 1)^2 + O(x^{-2})\right) \\ &= \frac{\beta - \alpha}{\pi} - \sum_{|k| \leq M} b_k \sum_{\rho}{}^{k} K(\rho - 1)^2 + O(x^{-2}) \cdot \sum_{|k| \leq M} b_k \\ &= \frac{\beta - \alpha}{\pi} - \sum_{|k| \leq M} b_k \sum_{\rho}{}^{k} K(\rho - 1)^2 + o(x^{-1}), \end{aligned} \tag{3.8}$$

where we have used our choice of $M = x^{1+\varepsilon}$. We now wish to provide a tight bound on the sum in (3.8). We now prove the central lemma in our estimate:

Lemma 3.5. *We have that for sufficiently large x,*

$$\sum_{|k|\leq M}\sum_{\rho}^{k}|K(\rho-1)|^2 < \frac{9}{10}.$$

Proof. First, notice that since ξ_E^k has infinite order for any $k \neq 0$, we may apply Lemma 2.1 without consideration of Siegel zeros. Now, let $B_1 = A - 2$ and $M = x^{1+\varepsilon}$ as before, set $T = M^2 = x^{2+2\varepsilon}$, and let $B_2 = B_1 - (2+2\varepsilon)c_4$ (see Lemma 2.3 for the definition of c_4) and assume $B_2 > 0$ (by selecting A large enough). We begin by computing the following Stieltjes integral over λ using the bounds given by Lemmas 2.3 and 3.1, the former of which will apply if we take x sufficiently large so that $T > \boldsymbol{N}(\mathfrak{m})(M+1)$:

$$\begin{aligned}\int_a^b x^{-B_1\lambda}\,dN(\lambda,T) &= x^{-B_1\lambda}N(\lambda,T)\big|_a^b + B_1\log x\int_a^b N(\lambda,T)x^{-B_1\lambda}\,d\lambda\\ &\leq \left|x^{-B_1 a}\cdot T^{c_4 a}\right| + \left|x^{-B_1 b}\cdot T^{c_4 b}\right| + \left|B_1\log x\cdot\int_a^b T^{c_4\lambda}x^{-B_1\lambda}\,d\lambda\right|\\ &= x^{-B_2 a} + x^{-B_2 b} + B_1\log x\left|\int_a^b x^{-B_2\lambda}d\lambda\right|\\ &\leq \frac{B_1+B_2}{B_2}\left(x^{-B_2 a}+x^{-B_2 b}\right).\end{aligned} \tag{3.9}$$

We will now bound the contribution of zeros in the rectangle defined by $1-c_3 < \beta < 1$ and $|\gamma| < T$ using (3.9). We first need to choose a, b appropriately. Applying the zero-free region stated in Lemma 2.1 to $L\left(s, \xi_E^k\right)$, we can pick

$$a = \frac{c_1}{\log \mathfrak{q}\left(iT, \xi_E^k\right)} \quad \text{and} \quad b \to \infty.$$

Given our choices of T and M as well as the fact that $|k| \leq M$, we deduce from (2.1) $\log \mathfrak{q}\left(iT, \xi_E^k\right) < C\log x$ for some absolute constant $C > 0$. Substituting these choices of a, b into (3.9), we find that for sufficiently large x, the contribution of zeros in this rectangle is at most B_3, where

$$B_3 := \frac{B_1+B_2}{B_2}\left(\exp\left(-\frac{B_2 c_1}{C}\right)\right). \tag{3.10}$$

Next, we bound the contribution of zeros in the rectangle $0 < \beta < 1 - c_3$ and $|\gamma| < T$; we show that it yields a negligible contribution of $o(1/x)$. The contribution of each zero with $\beta < 1-c_3$ is at most $x^{-B_1 c_3}$ by Lemma 3.1. Therefore, if we sum over zeros in vertical strips $[t-1, t+1]$ for $t = 0, 1, \ldots, T$ and appeal to Lemmas 2.2 and 3.1, we obtain the bound

$$\begin{aligned}\sum_{|k|\leq M}\sum_{\substack{0<\beta<1-c_3\\ |\gamma|<T}}|K(\rho-1)|^2 &\ll M\cdot\sum_{t=0}^{T}x^{-B_1 c_3}\log x\\ &\ll MTx^{-B_1 c_3}\log x\\ &\ll x^{3+3\varepsilon-B_1 c_3}\log x,\end{aligned}$$

which is $o(1/x)$ as long as $B_1 = A - 2$ is sufficiently large. Finally, we will show that the contribution of zeros with $|\gamma| \geq T$ is also negligible. By Lemmas 2.2 and 3.1, this contribution is

$$\begin{aligned}\sum_{|k|\leq M}\sum_{\rho}^{k}\frac{4x^{-B_1(1-\beta)}}{|\rho-1|^2(\log x)^2} &\ll \sum_{|k|\leq M}\sum_{\rho}^{k}\frac{1}{|\rho-1|^2(\log x)^2}\\ &\ll \frac{1}{(\log x)^2}\sum_{|k|\leq M}\sum_{t>T}\frac{\log(kt)}{t^2}\\ &\ll \frac{M\log T}{T(\log x)^2},\end{aligned}$$

which is $o(1/x)$. In the last step above, we used the fact that $k \leq M \leq T$ and bounded the sum over t with an integral. To obtain the lemma, we simply need to select A in such a way that $B_3 < 9/10$, which is possible because B_3 can be made arbitrarily small by taking A sufficiently large. □

3.5 Completing the Proof

For convenience, put $\tau = \frac{\beta-\alpha}{\pi} \leq 1$. Observing that $\frac{2}{M+1} = O(x^{-1-\varepsilon}) = o(x^{-1})$ and recalling our bound on S, we see that

$$\begin{aligned}S &\geq \tau - \sum_{|k|\leq M} b_k \sum_{\rho}^{k} K(\rho-1)^2 + o(x^{-1})\\ &\geq \tau - \left(\tau + \frac{2}{M+1}\right)\sum_{|k|\leq M}\sum_{\rho}^{k}|K(\rho-1)|^2 - o(x^{-1})\\ &\geq \tau - \left(\tau + \frac{2}{M+1}\right)\left(\frac{9}{10} + o(x^{-1})\right) - o(x^{-1})\\ &\geq \frac{1}{10}\tau - o(x^{-1}).\end{aligned}$$

As $x = \pi \boldsymbol{N}(\mathfrak{m})/\tau$, it follows that $S > 0$ for x sufficiently large. Using our definitions of S in (3.2) and R in (3.3), it follows that there exists a $\mathfrak{p}$ such that $f_{\mathfrak{p}} = 1$, $\theta_{\mathfrak{p}} \in [\alpha, \beta]$ and $\boldsymbol{N}(\mathfrak{p}) \in [x^{A-2}, x^A]$. Since $f_{\mathfrak{p}} = 1$, we can write $\mathfrak{p} = (p)$ for a rational prime p. We then have that $\theta_{\mathfrak{p}} = \theta_p$, from which we deduce that

$$\theta_p = \theta_{\mathfrak{p}} \in [\alpha, \beta] \quad \text{and} \quad p \leq x^A.$$

This completes the proof of the main result, Theorem 1.1.

Remark. Notice that if a rational prime p is inert in $\mathcal{O}_K$, then $a_E(p) = 0$, so that $\theta_p = \pi/2$. Thus, whenever $\pi/2 \in I$, we have that all inert primes $p \nmid N_E$ satisfy $\theta_p \in I$. Thus, in this case, the bound in Theorem 1.1 can be improved substantially. In particular, the bound no longer depends on the length $\beta - \alpha$ of the interval I. □

Endnotes

[1] The kernel, as defined in §7 of [4] is missing a factor of s in the denominator. We have corrected the kernel in our definition of $K(s)$.

[2] This bound, as stated in (22) of [4], has an extraneous minus sign in the exponent of x. We have corrected the statement in Lemma 3.1.

[3]In performing an analogous calculation, Kaufman shifts the contour to $\sigma = -3/2$ (see [8]), but this is not possible because for a Hecke Grössencharakter ξ with frequency 1, the logarithmic derivative of $L(s+1,\xi)$ has a pole at $s = -3/2$.

Acknowledgements
This research was supervised by Ken Ono at the Emory University Mathematics REU and was supported by the National Science Foundation (grant number DMS-1250467). We would like to thank Ken Ono and Jesse Thorner for offering their advice and guidance and for providing many helpful discussions and valuable suggestions on the paper. We would also like to thank Professor Jean-Pierre Serre for pointing us to the reference [9]. Finally, we would like to thank the referees for their helpful comments.

Author details
[1]Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139, United States of America. [2]Department of Mathematics, Princeton University, Princeton, NJ, 08544, United States of America. [3]Department of Mathematics, Harvard College, Cambridge, MA 02138, United States of America.

Received: 30 June 2015 Accepted: 16 October 2015
Published online: 29 December 2015

References

1. Barnet-Lamb, T, Geraghty, D, Harris, M, Taylor, R: A family of calabi-yau varieties and potential automorphy II. Publ. Res. Inst. Math. Sci. **47**(1), 29–98 (2011)
2. Cojocaru, AC: Questions about the reductions modulo primes of an elliptic curve. In: Number theory, CRM Proc. Lecture Notes, vol. 36, pp. 61–79. Amer. Math. Soc., Providence, RI, (2004)
3. Fogels, E: On the zeros of *L*-functions. Acta Arith. **11**, 67–96 (1965)
4. Graham, S: On Linnik's constant. Acta Arith. **39**(2), 163–179 (1981)
5. Iwaniec, H: Topics in classical automorphic forms (graduate studies in mathematics, v. 17). American Mathematical Society, Providence, RI (1997). http://amazon.com/o/ASIN/0821807773/
6. Iwaniec, H, Kowalski, E: Analytic number theory. In: American Mathematical Society Colloquium Publications. vol. 53. American Mathematical Society, Providence, RI, (2004)
7. Jutila, M: A new estimate for Linnik's constant. Ann. Acad. Sci. Fenn. Ser. A I No. **471**, 8 (1970)
8. Kaufman, RM: The geometric aspect of Ju. V. Linnik's theorem on the least prime. Litovsk. Mat. Sb. **17**(1), 111–114 (1977)
9. Koval'čik, FB: Density theorems for sectors and progressions. Litovsk. Mat. Sb. **15**(4), 133–151 (1975)
10. Lemke Oliver, R, Thorner, J: Effective log-free zero density estimates for automorphic L-functions and the Sato-Tate conjecture (2015). arXiv e-prints available at 1505.03122
11. Linnik, YV: On the least prime in an arithmetic progression. I. The basic theorem. Rec. Math. [Mat. Sbornik] N.S. **15**(57), 139–178 (1944)
12. Linnik, YV: On the least prime in an arithmetic progression. II. The Deuring-Heilbronn phenomenon. Rec. Math. [Mat. Sbornik] N.S. **15**(57), 347–368 (1944)
13. Montgomery, HL: Ten lectures on the interface between analytic number theory and harmonic analysis. In: CBMS Regional Conference Series in Mathematics. vol. 84. Amer. Math. Soc, Providence, RI, (1994)
14. Ono, K: The web of modularity: arithmetic of the coefficients of modular forms and *q*-series. In: CBMS Regional Conference Series in Mathematics. vol. 102. Amer. Math. Soc., Providence, RI, (2004)
15. Silverman, JH: Advanced topics in the arithmetic of elliptic curves. In: Graduate Texts in Mathematics. vol. 151. Springer-Verlag, New York, (1994). http://dx.doi.org/10.1007/978-1-4612-0851-8
16. Weil, A: Jacobi sums as "Grössencharaktere". Trans. Amer. Math. Soc. **73**, 487–495 (1952)